UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,722	03/24/1999	DAVID A. LEE	042390.P6526	1130

7590 08/10/2005

WILLIAM W SCHAAL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
GYORFI, THOMAS A	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/275,722	LEE, DAVID A.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☒ Claim(s) *19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 remain for examination. The correspondence filed 5/27/05 amended claims 1, 11, and 16.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/27/05 has been entered.

Response to Arguments

3. Applicant's arguments filed 5/27/05 have been fully considered but they are not persuasive.

Applicant argues, "*It is respectfully asserted that, as just one example of how the text cited by the PTO fails to meet the language of the rejected claims. Lotspiech does not show, teach, use, or describe utilizing matrix keys of at least two selected columns of the key matrix to produce a secret device key. The PTO states that Lotspiech shows this feature on Column 5, lines 55-68, but Applicant respectfully asserts that Lotspiech does not show this.*" Examiner disagrees with this contention. The cited paragraphs further states that the session number is encrypted multiple times using multiple device keys (lines 63-65). In embodiments of the Lotspiech disclosure where $M \geq 2$, then it necessarily follows that the result is derived from elements of at least

two columns (see also Figure 3). In addition, the keys $S_{j,l}$ initially selected for further processing can come from an arbitrary number of rows and columns (see the example on col. 5, lines 42-54), and thus there exists embodiments of the Lotspeich disclosure wherein the results are derived from at least two rows and/or two columns of the matrix.

Claim Objections

4. Claim 19 is objected to because of the following informalities: there appears to be no antecedent basis for the limitation "machine readable medium". The only disclosure Examiner could determine to be of any relevance pertains to the memory of the certification authority (page 9, lines 1-22), but it would appear that this passage only supports storing keys in this memory, and not computer programs to implement a method using said keys. Examiner respectfully submits that appropriate correction or clarification is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As currently recited, the methods fail to result in a practical application in the useful arts which when executed produces a useful, concrete and tangible result. As written, the key is not necessarily produced in such a

manner that a machine would be able to utilize it and realize its functionality absent further processing. Further, the method could be implemented using pen and paper.

Claim Rejections - 35 USC § 102

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1, 3-11, and 13-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Lotspiech (U.S. Patent 6,118,873).

Referring to Claim 1:

Lotspiech discloses a method comprising: providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2 (Fig 3; col. 5, lines 5-20); dedicating the rows of the matrix to a first classification (col. 2, lines 40-60; col. 5, lines 30-40; Fig. 3, sets); for each column of the key matrix to produce a secret device key which is part of a first set of secret device keys (col. 5, lines 42-68; col. 6, lines 30-40; Fig. 3, sets); and producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys (col. 6, lines 25-42).

Referring to Claim 3:

Lotspiech discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses prior to performing the arithmetic operations, the method comprises: generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys (col. 5, lines 55-68).

Referring to Claim 4:

Lotspiech discloses the limitations as discussed in Claim 3 above. Lotspiech further discloses the key selection vector is uniquely assigned to a first digital platform (col. 5, lines 60-65).

Referring to Claim 5:

Lotspiech discloses the limitations as discussed in Claim 4 above. Lotspiech further discloses wherein prior to producing the shared secret key, the method comprises: receiving a key selection vector from a second digital platform in communication with the first digital platform (col. 5, lines 40-50); and analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys (col. 5, lines 10-30, 40-65).

Referring to Claims 6 and 16:

Lotspiech discloses the limitations as discussed in Claims 1 and 11 above. Lotspiech further discloses prior to performing arithmetic operations on keys of at least two selected rows, the method further comprises dedicating the rows of the key matrix to a first classification, and dedicating the columns of the key matrix to a second classification (col. 5, lines 30-40; Fig. 3; index).

Referring to Claim 7:

Lotspiech discloses the limitations as discussed in Claim 6 above. Lotspiech further discloses first classification includes digital platforms designed to provide information to other digital platforms (col. 4, lines 45-65).

Referring to Claim 8:

Lotspiech discloses the limitations as discussed in Claim 7 above. Lotspiech further discloses the second classification includes digital platforms designed to receive information from other digital platforms (col. 4, lines 45-65).

Referring to Claim 9:

Lotspiech discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses producing of the shared secret key comprises: analyzing contents of an incoming key selection vector (col. 6, lines 30-35); and performing arithmetic

operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector (col. 6, lines 35-40).

Referring to Claim 10:

Lotspiech discloses the limitations as discussed in Claim 9 above. Lotspiech further discloses the producing of the shared secret key further comprises: performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector (col. 6, lines 34-40).

Referring to Claim 11:

Lotspiech discloses a method comprising providing a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and $M \geq 2$ (Fig 3; col. 5, lines 5-20); dedicating the rows of the matrix to a first classification (col. 2, lines 40-60; col. 5, lines 30-40); for each row of the key matrix, performing arithmetic operations utilizing matrix keys of at least two selected columns of the key matrix to produce a secret device key which is part of a first set of secret device keys (col. 5, lines 42-68); producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys (col. 6, lines 25-43).

Referring to Claim 13:

Lotspiech discloses the limitations as discussed in Claim 11 above. Lotspiech further discloses prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected columns of the key matrix from which to produce the first set of secret device keys (col. 5, lines 55-68).

Referring to Claim 14:

Lotspiech discloses the limitations as discussed in Claim 11 above. Lotspiech further discloses the key selection vector is uniquely assigned to a first digital platform (col. 5, lines 60-65).

Referring to Claim 15:

Lotspiech discloses the limitations as discussed in Claim 14 above. Lotspiech further discloses wherein prior to producing the shared secret key, the method comprises: receiving a key selection vector from a second digital platform in communication with the first digital platform (col. 5, lines 40-50); and analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys (col. 5, lines 10-30, 40-65).

Referring to Claim 17:

Lotspiech discloses the limitations as discussed in Claim 11 above. Lotspiech further discloses producing of the shared secret key comprises: analyzing contents of an incoming key selection vector (col. 6, lines 30-35); and performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector (col. 6, lines 35-40).

Referring to Claim 18:

Lotspiech discloses the limitations as discussed in Claim 17 above. Lotspiech further discloses the producing of the shared secret key further comprises: performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector (col. 6, lines 34-40).

Referring to Claim 19:

Lotspiech discloses a machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising: an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector (col. 6, lines 10-42); a transfer function to output at least a key selection vector assigned to the first digital platform (col. 6, lines 30-40); a hash function to perform a hash operation on at least the shared secret key to produce a resultant hash value (col. 6, lines 30-40); and a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector (col. 6, lines 30-40; col. 6, lines 20-30).

Referring to Claim 20:

Lotspiech discloses a network comprising: a first digital platform; and a certification authority in communication with the first digital platform (Fig 1; col. 5, lines 5-20), the certification authority having access to a key matrix featuring matrix keys arranged in accordance with at least a first dimension and a second dimension (col. 5, lines 30-50), generating a first key selection vector and providing a first set of secret device keys produced from selected matrix keys of the key matrix (col. 5, lines 40-50).

Referring to Claim 21:

Lotspiech discloses the limitations of Claim 20 above. Lotspiech further discloses a second digital platform in communication with the certification authority and the first digital platform (col. 6, lines 55-68; col. 8, lines 30-40), the second digital platform being uniquely assigned a second key selection vector indicating at least two grids of the key matrix (col. 6, line 60-col. 7, line 10) and a second set of secret device keys produced from matrix keys situated in at least two grids of the key matrix (col. 7, lines 10-25).

Referring to Claim 22:

Lotspiech discloses the limitations of Claim 21 above. Lotspiech further discloses the first and second digital platforms to exchange the first and second key selection vectors in order for each digital platform to produce a shared secret key to

ensure that communications between the first and second digital platforms are secure (col. 8, lines 30-45).

Referring to Claim 23:

Lotspiech discloses a certification authority comprising: a memory to store a key matrix having N rows and M columns of matrix keys, where N>_2 and M>_2 (Fig 1; Fig 3; col. 5, lines 10-20); a logic to generate a key selection vector for each digital platform registered with the certification authority (col. 5, lines 20-30, 40-50).

Referring to Claim 24:

Lotspiech discloses the limitations of Claim 23 above. Lotspiech further discloses the logic includes a processing unit (col. 4, lines 5-20).

Referring to Claim 25:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the processing unit produces a first set of secret device keys by performing arithmetic operations on matrix keys along selected columns of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform (col. 5, lines 50-68).

Referring to Claim 26:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the matrix keys along the processing unit performs arithmetic operations on matrix keys along selected rows of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform (col. 6, lines 30-45).

Referring to Claim 27:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the matrix keys are only known by the certification authority (col. 5, lines 15-20).

Claim Rejections - 35 USC § 103

9. Claims 2 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al. (U.S. Patent 6,118,873), and further in view of Luther (U.S. Patent 5,533,127).

Referring to Claims 2 and 12:

Lotspiech discloses the limitations as discussed in Claims 1 and 11 above.

Lotspiech does not explicitly disclose "the arithmetic operations include modular addition."

Luther further discloses the arithmetic operations include modular addition (col. 7, lines 35-50; Fig .9).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that arithmetic operation is modular addition. One of ordinary skill in the art would have been motivated to do this because it would provide a method for generating a common key (Lotspiech: col. 6, lines 35-42).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
7/27/05

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100